IN THE CLAIMS:

1-4 (Canceled)

5. (Original) A method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;

obtaining network information, from network equipment connected to the device, regarding the attack;

determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and

identifying a physical entry point associated with the logical entry point.

6. (Original) The method of claim 5, wherein the intrusion information includes an address.

7. (Currently Amended) The method of claim [[5]] 6, wherein the address is a source address.

8. (Currently Amended) The method of claim [[5]] 6, wherein the address is a destination address.

9. (Currently Amended) The method of claim [[5]] 6, wherein the network information includes a logical port identifier of a logical port associated with the address.

10. (Currently Amended) The method of claim 9, wherein the step of determining a logical entry point includes the step of finding, in the network data information, the logical port identifier of the logical port associated with the address.

11. (Original) The method of claim 9, wherein the step of identifying a physical entry point includes the step of identifying a physical port associated with the logical port.

12. (Canceled)

13. (Canceled)

14. (Canceled)

15. (Original) The method of claim 5, wherein the network equipment includes a firewall with routing function.

16. (Original) The method of claim 5, wherein the network equipment includes a network dispatcher.

17. (Original) The method of claim 5, wherein the network equipment includes a load balancer.

18. (Original) The method of claim 5, wherein the intrusion detection system includes network based intrusion detection equipment.

19. (Original) The method of claim 5, wherein the intrusion detection system includes host based intrusion detection equipment.

20. (Original) The method of claim 5, wherein the intrusion detection system includes application based intrusion detection equipment.

21. (New) A method of identifying the entry point of an attack upon a device protected by an intrusion detection system, said device one of a plurality of devices connected by a network, the method comprising the computer-implemented steps of:
    detecting an attack on the device;
    notifying a correlation engine of the attack on the device;
    obtaining intrusion information regarding the attack;
    obtaining network information regarding the attack;

using the correlation engine, correlating the intrusion information and the network
    information to produce correlation information;

using the correlation information, finding on the network a logical port of
    connection used by the attack; and

mapping the logical port on the network to a physical port on the network using
    the correlation engine.

22.   (New) The method of claim 21 comprising the further step of:
    alerting a network manager to the location of the logical port and of the physical
        port.

23.   (New) The method of claim 21 wherein the step of mapping is performed using
the correlation engine.

24.   (New) The method of claim 21 wherein:
    the intrusion information includes an address; and
    the network information includes a logical port identifier of a logical port
        associated with the address.

25.   (New) An apparatus for detecting a point of an attack on a network, the apparatus
comprising:

    network equipment for connecting a protected device to a network;

    an intrusion detection system comprising intrusion detection equipment;

    a correlation engine adapted to:

        receive a notification of an attack on the protected device;

        receive intrusion information regarding the attack;

        receive network information regarding the attack, wherein the
            network information pertains to the network;

        correlate the intrusion information and the network information to
            produce correlation information;

        find on the network a logical port of connection used by the attack;
            and

Page 4 of 9
Bardsley et al. – 09/917,368

map the logical port on the network to a physical port on the
network using the correlation engine.

26. (New) The apparatus of claim 25 further comprising:

means for alerting a network manager to the location of the logical port and of the
physical port.

27. (New) The apparatus of claim 25 wherein:

the intrusion information includes an address; and

the network information includes a logical port identifier of a logical port
associated with the address.

Page 5 of 9
Bardsley et al. – 09/917,368